Process and Apparatus for Improving the Security of Authentication Procedures Using a New "Super PIN"

BACKGROUND OF THE INVENTION

Field of the Invention

1. The present invention relates to apparatus and method for improving the security of authentication procedures using a new "Super PIN", particularly for protecting credit card and other purchase transactions.

Related Art

2. Authentication of users and systems began with the signature or seal. These methods are not very secure and principally rely on legal protections such as laws against forgery to ensure their effectiveness. The signature or seal has been mostly replaced by the use of secret passwords and Personal Identification Numbers (PINs) to authenticate users of systems and has been common practice for a number of years. These authentication systems have proven themselves and are widely used to authenticate people for systems ranging from computers to credit cards and telephone cards. It is also used for automated authentication of systems such as cellular telephones. The security of these systems is limited by the vulnerability of the system to the compromise of the password or PIN. But, it has an advantage over an ordinary signature in that it can be automatically processed.

The standard solution to this problem has been to move to a much more complicated system relying on smart cards to provide encryption or challenge/response security for authentication. This solution, while

very effective, is also quite expensive to deploy on a large scale. Individual cards must be issued and an infrastructure to process them.

3. Transaction security systems usually consist of a Unique Identifier that is used as a reference for the individual involved in a transaction (such as a credit card account number). This identifier is used to indicate the individual involved in the transaction. The most commonly used security solution is to augment the identifier is a Personal Identification Number (PIN). This Secret Identifier is entered into ATM machines or phones for transactions. The problem with this solution for many transactions is that the Secret Identifier may be disclosed - "shoulder surfing" is a major problem for phone cards. Without the use of a Secret Identifier, a Unique Identifier is not sufficient because it is widely distributed.

4. The next level of solution that has been proposed is to use a smart card to store or process Secret Identifier information so that it is only available to the issuer of the card or the card itself. The problem with this approach is that, while it is very secure, it is also expensive. Additional processing capability is required at the location of each transaction and someone must pay for the smart card, itself.

SUMMARY OF THE INVENTION

5. The "Super PIN" solution is a compromise that targets the most common forms of fraud - casual, low-tech criminals who steal individual cards at the time of a single transaction. This scenario matches theft by waiters, sales clerks, "shoulder surfing", "dumpster divers", and other

individuals that have incidental access to credit card numbers and PINs. This solution augments the Secret Identifier or PIN with a scheme that effectively obscures the PIN while being implementable without additional technology for the consumer, the point of sale system, or at the credit card server.

6. The "Super PIN" attempts to deal with the most common forms of fraud - the casual observance or theft of PINs or passwords. This solution is not as strong as a smart card encryption or challenge/response system, but it is radically cheaper. It builds on the traditional processing infrastructure with minimal increase in complexity and may even reduce processing requirements. On the customer side, the traditional PIN or password is augmented by a procedural change that should be easy for ordinary people to implement.

trade off

7. This solution works simply by "scrambling" the Secret Identifier with consumer generated random data to obscure the identifier. This scrambled identifier is included with the Unique Identifier to authenticate the transaction. The consumer will scramble his Secret Identifier with a new set of random data for each transaction. The credit card server can validate the Secret Identifier information by comparing it with its own stored copy of the information. The credit card server will reject multiple transactions that use the same scrambled identifier. The credit card server will also be suspicious of transactions that have "similar" scrambled identifiers to previously used ones. This has several benefits - the adversary cannot use the data that was given in identical format or similar format or he will have the transaction rejected and provide a good indicator of where the fraud occurred. An adversary will need to see multiple transactions

from the same account to be able to beat the system. This significantly increases the difficulty of casual fraud with only minimal cost impact to implement.

8. In accordance with a first aspect of the present invention, a method for a provider to verify a client's secret identifier, comprises the steps of: (i) the client scrambles his/her predetermined secret identifier in a random way with random data; (ii) the scrambled data is transmitted to the provider; and (iii) the provider determines whether the client's secret identifier is present in the received scrambled data. Preferably, the provider rejects the transaction if the random data in the received scrambled data is substantially the same as random data received in a previous transaction corresponding to said client.

9. In accordance with another aspect of the present invention, a method for a provider to verify a client's secret identifier received in scrambled data which includes the secret identifier scrambled with random data, comprises the steps of: (i) determining whether the client's secret identifier is present in the received scrambled data; (ii) comparing the random data in the received scrambled data with previously received random data corresponding to said client; and (iii) authorizing a transaction if the random data in the received scrambled data is substantially different from said previously received random data.

Brief Description of the Drawings

10. Figure 1 shows the client usage process, how a consumer or other user would participate in the Super PIN process.

11. Figure 2 shows a sample service "chit" to demonstrate how a client/consumer could easily implement this procedure using existing processes.

12. Figure 3 shows the process that is followed by an intermediary, such as a merchant, for processing a Super PIN protected transaction. Figure 4 shows the process that is followed by a provider, such as a credit card company, for validating a client/consumer's Super PIN.

Detailed Description of the Preferred Embodiments

Introduction

13. There are three major processes involved in the "Super PIN" - client usage, provider verification, and provider issuance. Client usage is the process that the Client uses to create the "Super PIN". Provider verification is the process used to verify the "Super PIN" including the special case where there is an intermediary (such as a merchant) and Provider Issuance is the process used to issue new or altered "Super PINs". The following are relevant terms:

- Unique Identifier - an account number, user ID, or other name used to uniquely track and identify people, equipment, or other items of interest;
- Secret Identifier - a secret set or sequence of symbols, such as a series of numbers or alphanumeric characters, associated with a given Unique Identifier. Passwords and PINs are examples of Secret Identifiers. Secret Identifiers may be periodically changed;

- Random Data - a set or sequence of symbols selected by some random or pseudo-random process;
- Super PIN - a combination of a given Secret Identifier and Random Data that are, in turn, put into a random sequence;
- Transaction - an activity that needs identification and authentication such as a session or purchase;
- Client - an individual person or system that participates in a transaction. A unique identifier is associated with each client; and
- Provider - an entity that authorizes a transaction such as a credit card firm, telephone company, or computer.

The example described in detail below is for a credit card processing scenario. Other scenarios would follow a similar general procedure.

The Preferred Embodiment

Client Usage

14. Prior to the beginning of any transaction, the Client will be provided with a Unique Identifier, a Secret Identifier, and the process for generating the Super PIN. For a credit card scenario, the Unique Identifier is the credit card number and the Secret Identifier is the PIN. The process for generating the Super PIN is described as follows (see Figure 1):

S1. Once the Client has decided to begin a transaction (in this case a credit card purchase), the Unique Identifier and purchase price information are recorded by the merchant on a chit. In traditional credit card processing, the Client would sign the chit. For the Super PIN process, the Client will also insert the Super PIN as described below. The chit will include spaces for the Super PIN.

S2. The Client will write in the symbols from his Unique Identifier into some of the spaces in arbitrary order and in arbitrary spaces.

S3. The Client will fill in the remaining spaces with Random Data - symbols created at random by the Client.

S4. The resulting scrambled Unique Identifier and Random Data are provided to the merchant (see Figure 2 for sample manual chit). The purchase is then either approved or denied by the Provider (see below).

Provider Verification

15. Providers authenticate clients by means of the Super PIN. Often, however, there is an intermediary (see Figure 3) in the verification process who communicates the information between the Client and the Provider, often for his own purposes, such as a merchant validating a credit card purchase.

Intermediary

16. The intermediary, if present, carries out the following processes (See Fig. 3):

S10. The intermediary receives the Unique Identifier and Super PIN from the Client.

S20. Optionally, the intermediary combines this information with any additional information, such as amount purchased for a credit card transaction.

S30. The intermediary communicates the Unique Identifier, Super PIN, and, optionally, other information, to the Provider.

S40. The intermediary receives a confirmation, denial, or other status information from the Provider.

Verification

17. Before any transaction, the Provider stores the Unique Identifier information and Secret Identifier for each Client (see Provider Issuance, below). The Provider may also store one or more of the previous Super PINs provided by the Client. The transaction processing by the Provider goes as follows (see Figure 4):

S41. The Provider receives the Unique Identifier information, Super PIN, and optionally additional information from the Client or intermediary.

S42. The Provider uses the Unique Identifier information to retrieve the Client's Secret Identifier from storage.

S43. The Provider reviews the Secret PIN received from the Client, symbol by symbol, to confirm if all of the symbols from the Secret Identifier are included.

S44 and S50. If they are not included, then the Provider takes appropriate action, likely including rejecting the continued processing of the transaction.

S45. If all of the symbols from the Client's Secret Identifier are included, the Provider may retrieve the set of previous Super PINs from storage.

S46. The Provider will then compare the previous Super PINs with the new Super PIN.

S47 and S51. If the new Super PIN is the same as a recent Super PIN, the Provider may have a good reason to reject the transaction or carry out further authentication. For credit card purchases, this could include running heuristic models of purchases or requesting photographic or other ID to be provided by the supposed Client.

S49 and S48. If the new Super PIN is very similar to a recent Super PIN (depending on whatever filter or analysis tool the Provider wishes to use), the Provider may also have good reason to reject the transaction or carry out further authentication.

S52. If the new Super PIN is not the same or very similar to recent Super PINs, the Provider will likely authorize the transaction.

Provider Issuance

18. The Provider uses some independent communications means to provide the Client with the Client's Unique Identifier and Secret Identifier. These may be provided separately as credit cards are often mailed separately from PINs. It is possible for the Provider to send the Client some unique process used to create the Super PIN as opposed to the standard Super PIN process described above.

Adversary Challenge

19. The difficulty an adversary faces is different from that he faces today. Today, if the adversary sees a Client's Secret Identifier, he can easily pretend to be the Client and carry out transactions until he is caught based upon some heuristic or other security system. In the Super PIN system, he sees the Secret Identifier, but cannot separate it from the Random Data. If he reuses the same Super PIN or set of symbols from the Super PIN, he will be caught since the Provider stores previously used Super PINs. If he changes any of the symbols in the Super PIN that he uses, he is as likely to guess what one of the symbols from the Secret Identifier is as he is to guess one that is from the Random Data. It is likely, but not required that the Secret Identifier and the Random Data both contain the same number of symbols. If the proposed Super PIN is very close to a previous Super PIN, it is

also quite likely to be rejected or include invalid guesses as to which symbols were from the Secret Identifier. The more "different" the Super PIN that the adversary uses, the more likely that it will be rejected for not including the Secret Identifier, but the more "similar" the Super PIN that the adversary used, the more likely that it will be rejected as a "re-use" or near re-use of a previous Super PIN. Clients are likely to pick very different Random Data - probably with worse correlation than at random, so it should be easy to build strong filters to separate Clients from adversaries.

20. The security of this system is focused on the low-tech or casual adversary. Once an adversary sees multiple Super PINs from the same Client, the Super PIN system becomes very easy to defeat very quickly. Such an adversary would need to monitor and analyze data from potential victims to be successful - but such adversaries often have other means of defeating security systems.

21. The following are some potential applications for the Super PIN system:

- Internet Transactions - the speed and cost of processing for the Super PIN is significantly lower than for cryptographic and other security systems. The system can also be augmented by having the client's local computer generate the Random Data and scramble the Secret Identifier and Random Data (this can be done by the person manually, as well).
- Computer and Network Logins - the user can enter his Super PIN into the keyboard or keypad.

- Building Security - replacing PIN codes for door, garage, room, or other entry systems.
- Telephone Cards - the user can state or type his Super PIN into the phone.
- Credit Card and ATM Systems - this can even be used with manual "chits" where the user can write the Super PIN above his signature and it can be processed by traditional credit card systems with minimal change. This system should run much faster than the heuristics that are used to profile card users and so could be an effective "first filter" in the transaction authorization process.
- Cellular Phones - today have a "secret ID" that is sent to the base station. This can and has been collected via monitoring of electronic signals. The Super PIN could be used and would force the adversary to collect the same phone on multiple calls - significantly more complicated than today, yet much faster for the legitimate system to process.
- It is also possible to use alternate "rules" for the creation of the Super PIN.
- There are better and worse choices for symbol sets (numeric, alphanumeric, ASCII characters, UNICODE characters, etc.), number of symbols in the Secret Identifier, and size of Secret Identifier vs. Random Data to give a significant range of security characteristics for a Super PIN system designer.

22. The individual components shown in outline or designated by blocks in the Drawings are all well-known in the security authentication arts, and their specific construction and operation are not critical to the operation or best mode for carrying out the invention.

23. While the present invention has been described with respect to what is presently considered to be the preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. To the contrary, the invention is intended to cover various modifications and equivalents arrangements included within the spirit and scope of the appended clients. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.